Clean Version Of The Pending Claims Under 37 C.F.R. 1.121(c)(3):

Claims 1-6 and 22-26, now pending, are submitted below in accordance with 37 C.F.R. §1.121(c)(3), which presents a clean version of the entire set of pending claims in this single amendment paper.

1. An assembly comprising:

a device constructed in a form factor of a PCMCIA card, the device having an interface to communicate with a storage card and memory to store user data; and

a removable storage card associated with a user that alternately enables access to the user data on the memory when interfaced with the device interface and disables access to the user data when removed from the device.

2. An assembly as recited in claim 1, wherein the storage card comprises a smart card.

3. An assembly as recited in claim 1, wherein the memory comprises flash memory.

4. An assembly as recited in claim 1, wherein the device stores a user's profile that can be used to configure a computer.

5. An assembly as recited in claim 1, wherein the storage card stores a passcode and access to the user data in the memory of the device is enabled upon

authentication of a user-supplied passcode to the passcode stored on the storage card.

6. An assembly as recited in claim 1, wherein the device stores a public key and the storage card stores a corresponding private key and access to the user data in the memory of the device is enabled upon verification that the public key and the private key are associated.

22. A computer system, comprising:

a computer having a PCMCIA device reader; and

a smart card secured memory assembly having a form factor of a PCMCIA card to compatibly interface with the PCMCIA device reader in the computer, the smart card secured memory assembly having data memory to store user data and a removable smart card that alternately enables access to the user data when present and disables access to the user data when removed.

23. A computer system as recited in claim 22, wherein the data memory comprises flash memory.

24. A computer system as recited in claim 22, wherein the smart card stores a passcode and is configured to authenticate a user-supplied passcode entered into the computer as a condition for enabling access to the user data.

25. A computer system as recited in claim 22, wherein:

the smart card stores a first key;

the data memory stores a second key that is associated with the first key; and

the smart card is configured to authenticate the second key from the data memory using the first key as a condition for enabling access to the user data.

26. A computer system as recited in claim 22, wherein:

the smart card stores a passcode and a private key of a public/private key pair;

the data memory stores a public key of the public/private key pair; and

the smart card is configured to authenticate a user-supplied passcode entered into the computer as a condition for enabling access to the private key and to authenticate the public key from the data memory using the private key as a condition for enabling access to the user data.